T1439 Lawful Intercept Abuse

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Date | Who | Current text | Proposed text | Final text |
| May 14, 2022 and July 27 | MV |  |  | Formatting changes (not shown), new text in red |
|  |  |  |  |  |

Description: An adversary may use the Lawful Intercept (LI) system to listen in IP/Voice communication of a user by unauthorized configuration of LI function.

Lawful Interception function (based on the law) is performed by a network operator/access provider/service provider (NWO/AP/SvP), making available certain information to a law enforcement monitoring facility.

The relevant functions are: The Mediation and Delivery Function (MDF) in the MNO network, and the Law Enforcement Monitoring Facility (LEMF) in the law enforcement entity domain. This threat also considers the unauthorized access to this function (MDF) when hosted outside the operator’s network. If a vendor/supplier has access to the mobile network, then it will be possible for them to manipulate this function and bypass the audit mechanisms in a way that the abuse is not detected by the MNO.

Labelling:

* Sub-techniques: None
* Applicable Tactics: collection

Metadata:

* Architecture Segment: OA&M
* Platform(s): Legal Intercept
* Access type required: Administrative access
* Data Sources:
* Theoretical/Proof of concept/Observed: Theoretical

Procedure Examples:

|  |  |
| --- | --- |
| **Name** | **Description** |
| Specific example if known |  |

Mitigations

|  |  |
| --- | --- |
| **ID** | **Use** |
| M1035 | Limit access to resource over network. Limit the Point of Interception to only UPF, UDM, AMD and SMF |
| M1047 | Monitor MDF activity, monitor configuration changes (Default and active) |
| M1022 | Limit file and permission changes |

Pre-Conditions

|  |  |
| --- | --- |
| **Name** | **Description** |
|  |  |

Critical Assets

|  |  |
| --- | --- |
| **Name** | **Description** |
| Subscriber’s data | User plane and control plane data |
| User subscription profile data | Subscriber's identities (e.g. SUPI), APN name, UE's IP address, QoS, etc.), network usage, charging data record. |

Detection

|  |  |
| --- | --- |
| **ID** | **Detects** |
| DS0022 | File access, creation, deletion, modification, meta data |
| DS0029 | Network traffic monitoring for connection creation, traffic flows and network traffic contents |
| DS0002 | Restrict User accounts to establish connections to AMDF from known legal entities (IP addresses, certificates, logon credentials etc.). Monitor and block attempted violations. |

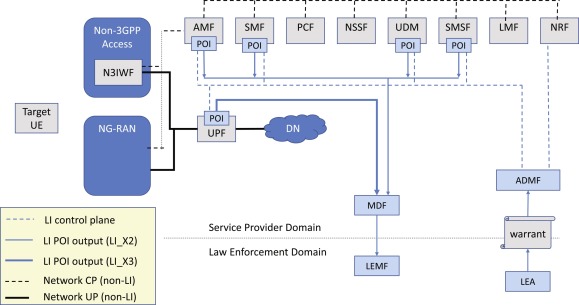
Post-Conditions

|  |  |
| --- | --- |
| **Name** | **Description** |
|  |  |

References

|  |  |
| --- | --- |
| Name | URL |
| European Union Agency for Cybersecurity (ENISA): “ENISA Threat Landscape for 5G Networks” Report, December 2020. | https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-for-5g-networks |
| R. Pell, S. Moschoyiannis, E. Panaousis, R. Heartfield, “Towards dynamic threat modelling in 5G core networks based on MITRE ATT&CK”, October 2021 | https://arxiv.org/abs/2108.11206 |

#doNotParse



The Mediation and Delivery Function (MDF) delivers the interception reports to the Law Enforcement Monitoring Facility (LEMF)

Law Enforcement Agency (LEA), which in general is the one that submits the warrant to the Service Provider. In some countries the warrant may be provided by a different legal entity (e.g. judiciary).

The Administration Function (ADMF), responsible for the overall management of the LI system. ADMF uses the LI\_X1 interface toward the 5GC NFs for managing the LI functionality.

Point of Interception (POI) is functionality that detects the target communication, derives the intercept related information or communications content from the target communications and delivers the output to the MDF. The POI is located in the relevant 5G NFs. The POI uses the LI\_X2 and LI\_X3 interfaces for delivering the interception product.

(from J.Guo): MDF often stays within the service provider domain, while LEMF will be on Law Enforcement domain.

The POI for MDF should be limited to UPF, UDM, AMD and SMF and no other functions